UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/709,423	05/05/2004	Chih-Chung Lu	IEIP0012USA	3422

27765 7590 04/23/2007 NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION P.O. BOX 506 MERRIFIELD, VA 22116	**EXAMINER** AVERY, JEREMIAH L

ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/23/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/23/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

winstonhsu.uspto@gmail.com
Patent.admin.uspto.Rcv@naipo.com
mis.ap.uspto@naipo.com.tw

PTOL-90A (Rev. 10/06)

Office Action Summary	Application No.	Applicant(s)
	10/709,423	LU, CHIH-CHUNG
	Examiner	Art Unit	
	Jeremiah Avery	2131	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 May 2004</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☒ Claim(s) *13 and 19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>05 May 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-20 have been examined.

Claim Objections

1.   Claim 13 is objected to because of the following informalities: grammatical error.

In claim 13, the Applicant claims "a I mask characteristic value set". The Examiner

recommends removing "I" from the sentence so as to better clarify the claim.

Appropriate correction is required.

2.   Claim 19 is objected to because of the following informalities: the limitation,

pertaining to "with regard to each of the specific IP address" is improper due to a lack of

plurality. The Examiner recommends making "address" plural so as to further clarify the

claim limitation. Appropriate correction is required.

Claim Rejections - 35 USC § 102

> (e) the invention was described in a patent granted on an application for patent by another filed in the
> United States before the invention thereof by the applicant for patent, or on an international application
> by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this
> title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act

of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior

to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by United

States Patent No. 6,691,168 to Bal et al., hereinafter Bal.

3.   Regarding claim 1, Bal teaches a method of speeding up packet filtering used in

a network security apparatus comprising:

generating a first hash space according to at least one rule used to filter the packets

received by the network security apparatus, and the first hash space presenting a mask

characteristic value set (Figures 4 and 11, column 2, lines 18-43, "a set of packet

filtering rules is first *divided* the rules into N dimensions" and "Each of the N dimensions

are then *divided* into a set of dimension rule ranges wherein each rule range defines a

non-overlapping contiguous range of values in a particular dimension and the rules that

may apply to packets that fall within that range", column 5, lines 51-60, "the rule space

is a two aspect/dimension rule space wherein each rule defines a two-dimensional

rectangle polytope. Thus, Rule A forms a first rectangle and Rule B forms a second

rectangle" and column 12, lines 5-21, "the rule set has been hashed by first examining

the two most significant bits (MSB) in the X dimension to select a particular search tree

to be used");

generating a second hash space according to at least one of the packets received by

the network security apparatus, and the second hash space with the same size as the

first hash space, presenting a packet characteristic value set (Figures 4 and 11, column

2, lines 18-43, "a set of packet filtering rules is first *divided* the rules into N dimensions"

and "Each of the N dimensions are then *divided* into a set of dimension rule ranges

wherein each rule range defines a non-overlapping contiguous range of values in a

particular dimension and the rules that may apply to packets that fall within that range",

column 5, lines 51-60, "the rule space is a two aspect/dimension rule space wherein

each rule defines a two-dimensional rectangle polytope. Thus, Rule A forms a first

rectangle and Rule B forms a second rectangle" and column 12, lines 5-21, "the rule set

has been hashed by first examining the two most significant bits (MSB) in the X

dimension to select a particular search tree to be used");

performing a specific Boolean operation with the first hash space and the second hash

space (Fig. 8, column 2, lines 44-52, "the output of each of the N search structures will

be an R-length bit vector. In such an embodiment, the N output bit vectors are logically

ANDed together to produce a final rule bit vector that is used to select the rule" and

column 7, lines 4-23, "assigned bit vectors from the different dimensions are then

logically ANDed together");

determining whether the packet characteristic value set is out of the mask characteristic

value set, according to the results of said Boolean operation, then it is decided whether

the packet is allowed to pass through the network security apparatus (Fig. 1, column 3,

lines 64-67, column 4, lines 1-3, "packet filtering can be used to provide security for a

local area network by filtering out packets from potential intruders" and lines 14-47,

"Internet gateway 130 may comprise a suite of firewall applications on a computer

system, a packet filtering router, or another type of network component that provides the

desired features" and "the Internet gateway 130 processes packets with a set of security

rules that screen out packets related to unauthorized actions", column 11, lines 54-67,

"In an Internet Protocol based packet filter, some of the fields that are examined are

defined with a value and a mask" and "The subnet mask defines the size of the network

in the least significant bits. The most significant bits in the network address value and

the least significant bits of the subnet mask value create contiguous ranges" and

column 12, lines 1-12).

4.   Regarding claim 2, Bal teaches wherein the network security apparatus

comprises a firewall so that the rule can be pre-installed in the firewall (Fig. 1, column 3,

lines 64-67, column 4, lines 1-3, "packet filtering can be used to provide security for a

local area network by filtering out packets from potential intruders" and lines 14-47,

"Internet gateway 130 may comprise a suite of firewall applications on a computer

system, a packet filtering router, or another type of network component that provides the

desired features" and "the Internet gateway 130 processes packets with a set of security

rules that screen out packets related to unauthorized actions", column 5, lines 63-67,

"pre-processes the rules" and column 6, lines 1-14).

5.   Regarding claim 3, Bal teaches wherein the firewall comprises a search filter

assisting the rule of the firewall to filter the packets (Fig. 1, column 3, lines 64-67,

column 4, lines 1-3, "packet filtering can be used to provide security for a local area

network by filtering out packets from potential intruders" and lines 14-47, "Internet

gateway 130 may comprise a suite of firewall applications on a computer system, a

packet filtering router, or another type of network component that provides the desired

features" and "the Internet gateway 130 processes packets with a set of security rules

that screen out packets related to unauthorized actions").

6.   Regarding claim 4, Bal teaches wherein the content of each rule comprises at

least a specific mask that needs to be filtered (Fig. 1, column 3, lines 64-67, column 4,

lines 1-3, "packet filtering can be used to provide security for a local area network by

filtering out packets from potential intruders" and lines 14-47, "Internet gateway 130 may

comprise a suite of firewall applications on a computer system, a packet filtering router,

or another type of network component that provides the desired features" and "the

Internet gateway 130 processes packets with a set of security rules that screen out

packets related to unauthorized actions", column 11, lines 54-67, "In an Internet

Protocol based packet filter, some of the fields that are examined are defined with a

value and a mask" and "The subnet mask defines the size of the network in the least

significant bits. The most significant bits in the network address value and the least

significant bits of the subnet mask value create contiguous ranges" and column 12, lines

1-12).

7.   Regarding claim 5, Bal teaches converting the specific mask in each rule into

binary codes (Figures 6 and 11, column 6, lines 51-67, column 7, lines 1-23 and Table

1, column 11, lines 54-67 and column 12, lines 1-25, "in masks where the ones of the

mask appear in the most significant bits (MSBs) and the zeros of the mask appear in

the (LSBs) the defined ranges will be contiguous");

converting each relative address with bit values "1" in the binary codes into a

corresponding address pointing to the first hash space in order to obtain a set of the

corresponding addresses, with regard to each said specific mask, pointing to the first

hash space (Figure 11, column 11, lines 54-67 and column 12, lines 1-25, "in masks

where the ones of the mask appear in the most significant bits (MSBs) and the zeros of

the mask appear in the (LSBs) the defined ranges will be contiguous");

collecting each set of the corresponding addresses pointing to the first hash space

together thereby presenting a mask characteristic value set with regard to all of said

specific masks in the first hash space (Figures 8, 11 and 13a, column 6, lines 1-14, "The

pre-processing is completed by creating a different data structure to be used for

searching each different dimension range. Examples of possible data structures include

look-up tables and organized data trees.", column 11, lines 54-67, "The network

address defines a set of most significant bits that define a network address that the IP

host address belongs to", column 12, lines 1-21, "a Patricia tree", column 14, lines 53-

67, "a connection cache entry may contain a source IP address, a destination IP

address" and column 15, lines 1-20).

[As it is known in the art, a "Patricia tree" is a type of set data structure used to

store a set of strings and for constructing associative arrays (e.g. a look-up table) and

contains large ranges of values. Further, it is known in the art that subnet masks

consist of a series of 1s, followed by 0s (both in binary). The 1s designate the network

portion part of an address, while the 0s designate the part pertaining to the host

address. A device views the network address and subnet mask in binary and to

ascertain which part of the address is the network address and which part is the host

address, a Boolean "AND" operation is performed.

Thus, Bal's disclosure of, inter alia, "in masks where the ones of the mask appear

in the most significant bits (MSBs) and the zeros of the mask appear in the (LSBs) the

defined ranges will be contiguous" as well as "contiguous value and mask dimension

may easily be searched using a Patricia tree" teaches the claimed invention.]

8.   Regarding claim 6, Bal teaches utilizing the relative address with bit values "1" in

the binary codes to be a key of at least a specific hash function, and then performing the

hash operation to obtain each corresponding address pointing to the first hash space

(Figures 11, 13a and 13b, column 6, lines 1-14, "The pre-processing is completed by

creating a different data structure to be used for searching each different dimension

range. Examples of possible data structures include look-up tables and organized data

trees.", column 11, lines 54-67, "The network address defines a set of most significant

bits that define a network address that the IP host address belongs to" and column 12,

lines 1-40, "contiguous value and mask dimension may easily be searched using a

Patricia tree", "the rule points can be hashed before a search tree is used.", "the rule set

has been hashed by first examining the two most significant bits (MSB) in the X

dimension to select a particular search tree to be used", "the various dimension values

can be concatenated together to generate a single key" and "the concatenated value

can be used as the key to search a search tree").

9.   Regarding claim 7, Bal teaches generating a first hash space, with regard to

each specific mask, having a specific mask characteristic value, according to each set

of the corresponding addresses pointing to the first hash space (Figures 4 and 11,

column 2, lines 18-43, "a set of packet filtering rules is first *divided* the rules into N

dimensions" and "Each of the N dimensions are then *divided* into a set of dimension rule

ranges wherein each rule range defines a non-overlapping contiguous range of values

in a particular dimension and the rules that may apply to packets that fall within that

range", column 5, lines 51-60, "the rule space is a two aspect/dimension rule space

wherein each rule defines a two-dimensional rectangle polytope. Thus, Rule A forms a

first rectangle and Rule B forms a second rectangle", column 11, lines 54-67 and

column 12, lines 1-21, "the rule set has been hashed by first examining the two most

significant bits (MSB) in the X dimension to select a particular search tree to be used");

totaling each bit value with the same address in each said first hash space having

specific mask characteristic value thereby presenting a mask characteristic value set

with regard to all of the specific masks in one first hash space (Figures 4 and 11,

column 2, lines 18-43, "a set of packet filtering rules is first *divided* the rules into N

dimensions" and "Each of the N dimensions are then *divided* into a set of dimension rule

ranges wherein each rule range defines a non-overlapping contiguous range of values

in a particular dimension and the rules that may apply to packets that fall within that

range", column 5, lines 51-60, "the rule space is a two aspect/dimension rule space

wherein each rule defines a two-dimensional rectangle polytope. Thus, Rule A forms a

first rectangle and Rule B forms a second rectangle", column 11, lines 54-67 and

column 12, lines 1-21, "the rule set has been hashed by first examining the two most

significant bits (MSB) in the X dimension to select a particular search tree to be used").

10.   Regarding claim 8, Bal teaches wherein each packet comprises at least an IP

address that needs to be checked (Figures 3 and 13a, column 5, lines 13-27, column

11, lines 54-64, column 14, lines 53-67, "a connection cache entry may contain a source

IP address, a destination IP address" and column 15, lines 1-20).

11.   Regarding claim 9, Bal teaches converting at least one IP address in each packet

into binary codes (Figures 6 and 11, column 6, lines 51-67, column 7, lines 1-23 and

Table 1, column 11, lines 54-67 and column 12, lines 1-25, "in masks where the ones of

the mask appear in the most significant bits (MSBs) and the zeros of the mask appear

in the (LSBs) the defined ranges will be contiguous");

converting each relative address with bit value "1" in the binary codes into a

corresponding address pointing to the second hash space thereby obtaining a set of

corresponding addresses, with regard to each said IP address, pointing to the second

hash space (Figures 6 and 11, column 6, lines 51-67, column 7, lines 1-23 and Table 1,

column 11, lines 54-67 and column 12, lines 1-25, "in masks where the ones of the

mask appear in the most significant bits (MSBs) and the zeros of the mask appear in

the (LSBs) the defined ranges will be contiguous");

collecting each set of the corresponding addresses pointing to the second hash space

together thereby presenting a packet characteristic value set with regard to the at least

one packet in the second hash space space (Figures 8, 11 and 13a, column 6, lines 1-

14, "The pre-processing is completed by creating a different data structure to be used

for searching each different dimension range. Examples of possible data structures

include look-up tables and organized data trees.", column 11, lines 54-67, "The network

address defines a set of most significant bits that define a network address that the IP

host address belongs to", column 12, lines 1-21, "a Patricia tree", column 14, lines 53-

67, "a connection cache entry may contain a source IP address, a destination IP

address" and column 15, lines 1-20).

[As it is known in the art, a "Patricia tree" is a type of set data structure used to

store a set of strings and for constructing associative arrays (e.g. a look-up table) and

contains large ranges of values. Further, it is known in the art that subnet masks

consist of a series of 1s, followed by 0s (both in binary). The 1s designate the network

portion part of an address, while the 0s designate the part pertaining to the host

address. A device views the network address and subnet mask in binary and to

ascertain which part of the address is the network address and which part is the host

address, a Boolean "AND" operation is performed.

Thus, Bal's disclosure of, inter alia, "in masks where the ones of the mask appear

in the most significant bits (MSBs) and the zeros of the mask appear in the (LSBs) the

defined ranges will be contiguous" as well as "contiguous value and mask dimension

may easily be searched using a Patricia tree" teaches the claimed invention.]

12.   Regarding claim 10, Bal teaches utilizing each said relative address with bit value

"1" in the binary codes to be a key of at least a specific hash function, and then

performing a hash operation thereby obtaining each corresponding address pointing to

the second hash space (Figures 11, 13a and 13b, column 6, lines 1-14, "The pre-

processing is completed by creating a different data structure to be used for searching

each different dimension range. Examples of possible data structures include look-up

tables and organized data trees.", column 11, lines 54-67, "The network address defines

a set of most significant bits that define a network address that the IP host address

belongs to" and column 12, lines 1-40, "contiguous value and mask dimension may

easily be searched using a Patricia tree", "the rule points can be hashed before a

search tree is used.", "the rule set has been hashed by first examining the two most

significant bits (MSB) in the X dimension to select a particular search tree to be used",

"the various dimension values can be concatenated together to generate a single key"

and "the concatenated value can be used as the key to search a search tree").

13.   Regarding claim 11, Bal teaches generating the second hash space, with regard

to each said IP address, having a specific IP address characteristic value, according to

each set of the corresponding addresses pointing to the second hash space (Figures 4

and 11, column 2, lines 18-43, "a set of packet filtering rules is first *divided* the rules into

N dimensions" and "Each of the N dimensions are then *divided* into a set of dimension

rule ranges wherein each rule range defines a non-overlapping contiguous range of

values in a particular dimension and the rules that may apply to packets that fall within

that range", column 5, lines 51-60, "the rule space is a two aspect/dimension rule space

wherein each rule defines a two-dimensional rectangle polytope. Thus, Rule A forms a

first rectangle and Rule B forms a second rectangle", column 11, lines 54-67, column

12, lines 1-21, "the rule set has been hashed by first examining the two most significant

bits (MSB) in the X dimension to select a particular search tree to be used", column 14,

lines 53-67, "a connection cache entry may contain a source IP address, a destination

IP address" and column 15, lines 1-20);

totaling each bit value with same address in each said second hash space having

specific IP address characteristic value thereby presenting a packet characteristic value

set with regard to the at least one packet in one second hash space (Figures 4 and 11,

column 2, lines 18-43, "a set of packet filtering rules is first *divided* the rules into N

dimensions" and "Each of the N dimensions are then *divided* into a set of dimension rule

ranges wherein each rule range defines a non-overlapping contiguous range of values

in a particular dimension and the rules that may apply to packets that fall within that

range", column 5, lines 51-60, "the rule space is a two aspect/dimension rule space

wherein each rule defines a two-dimensional rectangle polytope. Thus, Rule A forms a

first rectangle and Rule B forms a second rectangle", column 11, lines 54-67, column

12, lines 1-21, "the rule set has been hashed by first examining the two most significant

bits (MSB) in the X dimension to select a particular search tree to be used", column 14,

lines 53-67, "a connection cache entry may contain a source IP address, a destination

IP address" and column 15, lines 1-20).

14.   Regarding claim 12, Bal teaches when at least one of bit values of the results of

the Boolean operation in the first hash space and the second hash space is out of value

"0", it is ensured that the packet characteristic value set is out of the mask characteristic

value set and therefore the packet can be allowed to pass through the network security

apparatus (Fig. 1, column 3, lines 64-67, column 4, lines 1-3, "packet filtering can be

used to provide security for a local area network by filtering out packets from potential

intruders" and lines 14-47, "Internet gateway 130 may comprise a suite of firewall

applications on a computer system, a packet filtering router, or another type of network

component that provides the desired features" and "the Internet gateway 130 processes

packets with a set of security rules that screen out packets related to unauthorized

actions", column 11, lines 54-67, "In an Internet Protocol based packet filter, some of

the fields that are examined are defined with a value and a mask" and "The subnet

mask defines the size of the network in the least significant bits. The most significant

bits in the network address value and the least significant bits of the subnet mask value

create contiguous ranges" and column 12, lines 1-12, "the zeros of the mask appear in

the (LSBs)").

[It is known in the art that subnet masks consist of a series of 1s, followed by 0s

(both in binary). The 1s designate the network portion part of an address, while

the 0s designate the part pertaining to the host address.]

15.   Regarding claim 13, Bal teaches a method of speeding up packet filtering used in

a network security apparatus, including a method of generating a mask characteristic

value set with regard to all specific masks that need to be filtered, comprising the steps

of:

extracting each of the specific masks from at least one rule pre-installed in the network

security apparatus (Fig. 1, column 3, lines 64-67, column 4, lines 1-3, "packet filtering

can be used to provide security for a local area network by filtering out packets from

potential intruders" and lines 14-47, "Internet gateway 130 may comprise a suite of

firewall applications on a computer system, a packet filtering router, or another type of

network component that provides the desired features" and "the Internet gateway 130

processes packets with a set of security rules that screen out packets related to

unauthorized actions", column 5, lines 63-67, "pre-processes the rules", column 6, lines

1-14, column 11, lines 54-67, "mask definitions" and column 12, lines 1-21, "the rule

points can be hashed before a search tree is used");

converting each of the specific masks into binary codes (Figures 6 and 11, column 6,

lines 51-67, column 7, lines 1-23 and Table 1, column 11, lines 54-67 and column 12,

lines 1-25, "in masks where the ones of the mask appear in the most significant bits

(MSBs) and the zeros of the mask appear in the (LSBs) the defined ranges will be

contiguous");

converting each relative address with bit value "1" in the binary codes into a

corresponding address pointing to a hash space thereby obtaining a set of the

corresponding addresses, with respect to each specific mask, pointing to the hash

space (Figures 6 and 11, column 6, lines 51-67, column 7, lines 1-23 and Table 1,

column 11, lines 54-67 and column 12, lines 1-25, "in masks where the ones of the

mask appear in the most significant bits (MSBs) and the zeros of the mask appear in

the (LSBs) the defined ranges will be contiguous");

collecting the each set of the corresponding addresses pointing to the hash space

together thereby presenting a l mask characteristic value set with regard to all of the

specific masks in the hash space (Figures 8, 11 and 13a, column 6, lines 1-14, "The

pre-processing is completed by creating a different data structure to be used for

searching each different dimension range. Examples of possible data structures include

look-up tables and organized data trees.", column 11, lines 54-67, "The network

address defines a set of most significant bits that define a network address that the IP

host address belongs to", column 12, lines 1-21, "a Patricia tree", column 14, lines 53-

67, "a connection cache entry may contain a source IP address, a destination IP

address" and column 15, lines 1-20).

[As it is known in the art, a "Patricia tree" is a type of set data structure used to

store a set of strings and for constructing associative arrays (e.g. a look-up table) and

contains large ranges of values. Further, it is known in the art that subnet masks

consist of a series of 1s, followed by 0s (both in binary). The 1s designate the network

portion part of an address, while the 0s designate the part pertaining to the host

address. A device views the network address and subnet mask in binary and to

ascertain which part of the address is the network address and which part is the host

address, a Boolean "AND" operation is performed.

Thus, Bal's disclosure of, inter alia, "in masks where the ones of the mask appear

in the most significant bits (MSBs) and the zeros of the mask appear in the (LSBs) the

defined ranges will be contiguous" as well as "contiguous value and mask dimension

may easily be searched using a Patricia tree" teaches the claimed invention.]

16.   Regarding claims 14 and 18, Bal teaches utilizing each said relative address with

bit value "1" in the binary codes to be a key of at least a specific hash function, and then

performing a hash operation to obtain said corresponding address pointing to the hash

space (Figures 11, 13a and 13b, column 6, lines 1-14, "The pre-processing is

completed by creating a different data structure to be used for searching each different

dimension range. Examples of possible data structures include look-up tables and

organized data trees.", column 11, lines 54-67, "The network address defines a set of

most significant bits that define a network address that the IP host address belongs to"

and column 12, lines 1-40, "contiguous value and mask dimension may easily be

searched using a Patricia tree", "the rule points can be hashed before a search tree is

used.", "the rule set has been hashed by first examining the two most significant bits

(MSB) in the X dimension to select a particular search tree to be used", "the various

dimension values can be concatenated together to generate a single key" and "the

concatenated value can be used as the key to search a search tree").

17.   Regarding claim 15, Bal teaches generating a hash space, with regard to each

specific mask, having a specific mask characteristic value, according to each set of the

corresponding addresses pointing to the hash space (Figures 4 and 11, column 2, lines

18-43, "a set of packet filtering rules is first *divided* the rules into N dimensions" and

"Each of the N dimensions are then *divided* into a set of dimension rule ranges wherein

each rule range defines a non-overlapping contiguous range of values in a particular

dimension and the rules that may apply to packets that fall within that range", column 5,

lines 51-60, "the rule space is a two aspect/dimension rule space wherein each rule

defines a two-dimensional rectangle polytope. Thus, Rule A forms a first rectangle and

Rule B forms a second rectangle", column 11, lines 54-67, "mask definitions", column

12, lines 1-21, "the rule set has been hashed by first examining the two most significant

bits (MSB) in the X dimension to select a particular search tree to be used", column 14,

lines 53-67, "a connection cache entry may contain a source IP address, a destination

IP address" and column 15, lines 1-20);

totaling each bit value with the same address in each said hash space having specific

mask characteristic value thereby presenting a mask characteristic value set with regard

to all of the specific masks in one hash space (Figures 4 and 11, column 2, lines 18-43,

"a set of packet filtering rules is first *divided* the rules into N dimensions" and "Each of

the N dimensions are then *divided* into a set of dimension rule ranges wherein each rule

range defines a non-overlapping contiguous range of values in a particular dimension

and the rules that may apply to packets that fall within that range", column 5, lines 51-60, "the rule space is a two aspect/dimension rule space wherein each rule defines a two-dimensional rectangle polytope. Thus, Rule A forms a first rectangle and Rule B forms a second rectangle", column 11, lines 54-67, "mask definitions", column 12, lines 1-21, "the rule set has been hashed by first examining the two most significant bits (MSB) in the X dimension to select a particular search tree to be used", column 14, lines 53-67, "a connection cache entry may contain a source IP address, a destination IP address" and column 15, lines 1-20).

18.   Regarding claim 16, Bal teaches setting the bit values of all sets of the corresponding addresses pointing to the hash space to be "1" thereby presenting a mask characteristic value set with regard to all of the specific masks in the hash space (column 11, lines 54-67 and column 12, lines 1-25, "in masks where the ones of the mask appear in the most significant bits (MSBs) and the zeros of the mask appear in the (LSBs) the defined ranges will be contiguous").

19.   Regarding claim 17, Bal teaches a method of speeding up packet filtering used in a network security apparatus, including a method of generating a packet characteristic value set with regard to specific IP addresses that needs to be checked, comprising: extracting each specific IP address from at least one packet received from the network security apparatus (Figures 3 and 13a, column 5, lines 13-27, column 11, lines 54-64, column 14, lines 53-67, "a connection cache entry may contain a source IP address, a destination IP address" and column 15, lines 1-20);

converting the each specific IP address in each packet into binary codes (Figures 6 and

11, column 6, lines 51-67, column 7, lines 1-23 and Table 1, column 11, lines 54-67 and

column 12, lines 1-25, "in masks where the ones of the mask appear in the most

significant bits (MSBs) and the zeros of the mask appear in the (LSBs) the defined

ranges will be contiguous");

converting each relative address with bit value "1" in the binary codes into a

corresponding address pointing to a hash space in order to obtain a set of the

corresponding addresses, with regard to each of the specific IP addresses, pointing the

hash space (Figures 6 and 11, column 6, lines 51-67, column 7, lines 1-23 and Table 1,

column 11, lines 54-67 and column 12, lines 1-25, "in masks where the ones of the

mask appear in the most significant bits (MSBs) and the zeros of the mask appear in

the (LSBs) the defined ranges will be contiguous");

collecting all sets of the corresponding addresses pointing to the hash space together

thereby presenting a packet characteristic value set with regard to the packet in the

hash space (Figures 8, 11 and 13a, column 6, lines 1-14, "The pre-processing is

completed by creating a different data structure to be used for searching each different

dimension range. Examples of possible data structures include look-up tables and

organized data trees.", column 11, lines 54-67, "The network address defines a set of

most significant bits that define a network address that the IP host address belongs to",

column 12, lines 1-21, "a Patricia tree", column 14, lines 53-67, "a connection cache

entry may contain a source IP address, a destination IP address" and column 15, lines

1-20).

[As it is known in the art, a "Patricia tree" is a type of set data structure used to store a set of strings and for constructing associative arrays (e.g. a look-up table) and contains large ranges of values. Further, it is known in the art that subnet masks consist of a series of 1s, followed by 0s (both in binary). The 1s designate the network portion part of an address, while the 0s designate the part pertaining to the host address. A device views the network address and subnet mask in binary and to ascertain which part of the address is the network address and which part is the host address, a Boolean "AND" operation is performed.

Thus, Bal's disclosure of, inter alia, "in masks where the ones of the mask appear in the most significant bits (MSBs) and the zeros of the mask appear in the (LSBs) the defined ranges will be contiguous" as well as "contiguous value and mask dimension may easily be searched using a Patricia tree" teaches the claimed invention.]

20.   Regarding claim 19, Bal teaches generating a hash space, with regard to each of the specific IP address, having a specific IP address characteristic value, according to each set of the corresponding addresses pointing to the hash space (Figures 4 and 11, column 2, lines 18-43, "a set of packet filtering rules is first *divided* the rules into N dimensions" and "Each of the N dimensions are then *divided* into a set of dimension rule ranges wherein each rule range defines a non-overlapping contiguous range of values in a particular dimension and the rules that may apply to packets that fall within that range", column 5, lines 51-60, "the rule space is a two aspect/dimension rule space wherein each rule defines a two-dimensional rectangle polytope. Thus, Rule A forms a first rectangle and Rule B forms a second rectangle", column 11, lines 54-67, column

12, lines 1-21, "the rule set has been hashed by first examining the two most significant

bits (MSB) in the X dimension to select a particular search tree to be used", column 14,

lines 53-67, "a connection cache entry may contain a source IP address, a destination

IP address" and column 15, lines 1-20);

totaling each bit value with the same address in each said hash space having a specific

IP address characteristic value thereby presenting a packet characteristic value set with

regard to the at least one packet in the hash space (Figures 4 and 11, column 2, lines

18-43, "a set of packet filtering rules is first *divided* the rules into N dimensions" and

"Each of the N dimensions are then *divided* into a set of dimension rule ranges wherein

each rule range defines a non-overlapping contiguous range of values in a particular

dimension and the rules that may apply to packets that fall within that range", column 5,

lines 51-60, "the rule space is a two aspect/dimension rule space wherein each rule

defines a two-dimensional rectangle polytope. Thus, Rule A forms a first rectangle and

Rule B forms a second rectangle", column 11, lines 54-67, column 12, lines 1-21, "the

rule set has been hashed by first examining the two most significant bits (MSB) in the X

dimension to select a particular search tree to be used", column 14, lines 53-67, "a

connection cache entry may contain a source IP address, a destination IP address" and

column 15, lines 1-20).

21.   Regarding claim 20, Bal teaches setting the bit values of all sets of the

corresponding addresses pointing to the hash space to "1" in order to present the

packet characteristic value set (column 11, lines 54-67 and column 12, lines 1-25, "in

masks where the ones of the mask appear in the most significant bits (MSBs) and the

zeros of the mask appear in the (LSBs) the defined ranges will be contiguous").

Conclusion

22.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

23.   The following United States Patents are cited to further show the state of the art

with respect to packet filtering, such as:

United States Patent No. 6,157,955 to Narad et al., which is cited to show a

packet processing system including a policy engine having a classification unit.

United States Patent No. 6,415,329 to Gelman et al., which is cited to show a

method and apparatus for improving efficiency of TCP/IP protocol over high delay-

bandwidth network.

United States Patent No. 7,100,195 to Underwood which is cited to show

managing user information on an e-commerce system.

24.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Jeremiah Avery whose telephone number is (571) 272-

8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

25.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

26.   Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JLA

CHRISTOPHER REVAK
PRIMARY EXAMINER